1.10 Ejercicios

1. Calcular el centro de los siguientes grupos:
   (a) El grupo cuaterniónico o de Hamilton: $\mathcal{H} = \{\pm 1, \pm i, \pm j, \pm k\}$ donde la "tabla de multiplicación" de $\mathcal{H}$ está dada por
   $$i.j = -j.i = k \ ; \ jk = -kj = i \ ; \ ki = -ik = j \ ; \ i.i = j.j = k.k = -1$$
   (verificar primero que $\mathcal{H}$ es un grupo!)
   (b) El grupo dihedral: D_n con $n > 2$ (sug. considere por separado n par o impar). Recordamos que $D_n = \langle r, s \ / \ r^n = 1, \ s^2 = 1, \ rs = sr^{-1} \rangle$.
   (c) Calcular *todos* los subgrupos de $\mathcal{H}$. Ver que a pesar de que $\mathcal{H}$ no es conmutativo, todos sus subgrupos son invariantes. (nombre: un grupo con esa propiedad se llama Hamiltoniano).
2. Sea X un conjunto y G un grupo. Entonces $G^X = Func(X,G) = \{f : X \to G\}$ es un grupo con la multiplicación punto a punto inducida por la multiplicación de G, i.e. el producto de dos funciones se calcula como $(f.g)(x) := f(x).g(x)$. Si X y G son finitos, cuál es el orden de G^X en términos del orden de G y el cardinal de X? Sea $H_{x_0} \subset Func(X,G)$ el subconjunto formado por las funciones $f : X \to G$ tales $f(x_0) = e_G$, es H_{x_0} un subgrupo? Es normal? Sea $g \neq e_G$ y $H_{x_0,g} \subset Func(X,G)$ el subconjunto de funciones f que verifican $f(x_0) = g$, es $H_{x_0,g}$ un subgrupo?
3. Sea X y G como antes, $x_0 \in X$ y $ev_{x_0} : Func(X,G) \to G$ dado por
   $$ev_{x_0}(f) := f(x_0)$$
   donde $f : X \to G$. Verificar que es un morfismo de grupos. Calcular núcleo e imagen.
4. Sean K y G dos grupos, y $\mathrm{Hom}_{Gr}(K,G)$ el subconjunto de $Func(K,G)$ formado por las funciones que son morfismos. ¿Es un subgrupo? Responder la pregunta para el caso G conmutativo y para el caso G no conmutativo.
5. Sea $f : G \to G'$ con G' abeliano. Ver que necesariamente $[G,G] \subseteq \mathrm{Ker}(f)$.
6. Si G es un grupo cualquiera, ver que la función
   $$\begin{aligned} ev_1 : \mathrm{Hom}_{Gr}(\mathbb{Z}, G) &\to G \\ f &\mapsto f(1) \end{aligned}$$
   es biyectiva.
7. Sea G un grupo **abeliano**. Considerar el grupo $(\mathbb{Z} \oplus \mathbb{Z})$ que consiste en $\mathbb{Z} \times \mathbb{Z}$ como conjunto y donde la suma está definida coordenada a coordenada. Ver que la función
   $$\begin{aligned} \mathrm{Hom}_{Gr}(\mathbb{Z} \oplus \mathbb{Z}, G) &\to G \times G \\ f &\mapsto (f(1,0), f(0,1)) \end{aligned}$$
   es una biyección. ¿es cierto el enunciado anterior si se cambia G abeliano por G no abeliano? Dar una demostración o un contraejemplo según el caso.
8. Ver que $\mathrm{Hom}_{Gr}(\mathbb{Q}, \mathbb{Z})$ sólo contiene el morfismo nulo.
9. ¿Es la función $f : \mathcal{H} \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$ definida por
   $$f(\pm 1) = (0,0) \ ; f(\pm i) = (1,0) \ ; f(\pm j) = (0,1) \ ; f(\pm k) = (1,1)$$
   un morfismo de grupos? En tal caso calcule núcleo e imagen.
10. ¿Existe un isomorfismo de grupos entre:
    (a) $\mathbb{Z}_4 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$?
    (b) $\mathbb{Z}_{2n} \cong D_n$?
    (c) $\mathbb{Z}_8 \cong \mathbb{Z}_4 \oplus \mathbb{Z}_2 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \cong \mathcal{H} \cong D_4$?
    (d) $(\mathbb{R}, +) \cong (\mathbb{R}_{>0}, .)$?
    (e) $(\mathbb{R}, +) \cong (\mathbb{R} - \{0\}, .)$?
11. Sean $m, n \in \mathbb{N}$ coprimos, ver que $\mathrm{Hom}_{Gr}(\mathbb{Z}_m, \mathbb{Z}_n)$ contiene sólo al morfismo nulo.
12. Sea k un cuerpo, ver que $det : GL_n(k) \to (k^*, .)$ es un morfismo de grupos, por lo tanto $Sl_n(k) := \{A \in k^{n \times n} \ / \ det(A) = 1\}$ es un subgrupo (invariante) de $GL_n(k)$. ¿Cuánto vale $GL_n(k)/Sl_n(k)$?
13. Calcular el orden de $Sl_2(\mathbb{Z}_3)$. Sugerencia: para hacer cuentas, escribir a $\mathbb{Z}_3$ como $\{\overline{0}, \overline{1}, \overline{-1}\}$). Describir el centro, y encontrar las clases de conjugación.
14. Sea H un subgrupo discreto de $(\mathbb{Q}, +)$. Ver que es cíclico, por lo tanto $H = \frac{m}{n}.\mathbb{Z}$ para un (único a menos de signo) racional $\frac{m}{n}$.

15. Sea H un subgrupo de $\mathbb{Q}$ finitamente generado. Demostrar que H es cíclico. Concluir que $\mathbb{Q}$ no es finitamente generado.
16. Ver que $\mathcal{S}_3 \cong D_3$.
17. Ver que el grupo de isometrías del tetrahedro es isomorfo a S_4.
18. Calcular el centralizador de $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ en $Sl_2(\mathbb{Z}_3)$ y en $GL_2(\mathbb{Z}_3)$.
19. Sea G un grupo, ver que la aplicación $G \to \mathrm{Aut}_{Gr}(G)$, $g \mapsto g.-.g^{-1}$ $(x \mapsto g.x.g^{-1})$ es un morfismo de grupos. Si además H es un subgrupo de G, ver que el morfismo de grupos $G \to \mathrm{Aut}_{Gr}(H)$ con la misma fórmula que el anterior queda bien definido $\Leftrightarrow$ H es un subgrupo invariante.
20. *Producto semidirecto.* Sean H y K dos grupos y $\phi : K \to \mathrm{Aut}_{Gr}(H)$ un morfismo de grupos, es decir, K actúa (multiplicativamente) sobre H (por ejemplo si H y K son dos subgrupos de un grupo G, $H \triangleleft G$ y $K \to \mathrm{Aut}_{Gr}(H)$, $k \mapsto k.-.k^{-1}$). Se define sobre el conjunto $H \times K$ la operación:

    $$(h,k).(h'.k') := (h.(\phi(k))(h'), k.k')$$

    (en el ejemplo entre paréntesis sería $(h,k).(h'.k') = (h.(k.(h').k^{-1}), k.k')$).

    (a) Probar que con esa operación, $H \times K$ tiene una estructura de grupo, que llamaremos **producto semidirecto** de H y K y notaremos $H \rtimes K$ (o $H \rtimes_\phi K$).

    (b) Encontrar el inverso de (h, e_K), el inverso de $(1_H, k)$, y el inverso de un (h,k) cualquiera.

    (c) Probar que el conjunto $H \times \{1_K\}$ es un subgrupo (isomorfo a H) invariante en $H \rtimes K$, más aún $(1_H, k)(h, 1_K)(1_H, k)^{-1} = ((\phi(k))(h), 1_K)$ (notar que esta igualdad es obvia para el ejemplo entre paréntesis).

    (d) Ver que la función $\pi : H \rtimes K \to K$ definida por $\pi(h,k) = k$ es un morfismo de grupos. Verificar que $\mathrm{Ker}(\pi) = H \times \{1_K\}$ (otra manera de ver que es invariante).

    (e) ¿Es siempre $\{1_H\} \times K$ invariante en $H \rtimes K$?

    (f) Sea G grupo y $\pi : G \to K$ un morfismo sobreyectivo (por lo tanto $K \cong G/\mathrm{Ker}(\pi)$) y sea $H = \mathrm{Ker}(\pi)$. Demostrar que *si existe* un morfismo de grupos $j : K \to G$ tal que $\pi(j(k)) = k$ $\forall k \in K$ entonces $G \cong H \rtimes K$.

    (g) $\{1_H\} \times K$ es invariante en $H \rtimes K$ $\Leftrightarrow$ los elementos de $H \times \{1_K\}$ conmutan con los elementos de $\{1_H\} \times K$.

    (h) Ver que $(-)^n : S^1 \to S^1$ $(z \to z^n)$ es un epimorfismo con núcleo G_n, pero S^1 *no* es isomorfo ni a $G_n \rtimes S^1$ ni a $S^1 \rtimes G_n$ para ninguna acción de S^1 sobre G_n ni de G_n sobre S^1.

21. Caracterizar $\mathrm{Hom}_{Gr}((\mathbb{Z}_n,+),(\mathbb{Z}_n,+))$, ¿cuales de esos morfismos son isomorfismos? caracterizar $\mathrm{Aut}_{Gr}((\mathbb{Z}_n,+))$.
22. Ver que $\mathcal{S}_3 \cong D_3 \cong \mathbb{Z}_3 \rtimes \mathbb{Z}_2$ para una acción adecuada de $\mathbb{Z}_2$ sobre $\mathbb{Z}_3$.
23. Demostrar que $\mathcal{S}_n/A_n \cong \mathbb{Z}_2$, más aún, $\mathcal{S}_n \cong A_n \rtimes \mathbb{Z}_2$.
24. Ver que $\mathrm{Aut}_{Gr}((\mathbb{Z}_n,+)) \cong (\mathcal{U}(\mathbb{Z}_n),.)$ (las unidades de $\mathbb{Z}_n$). Verificar que $|\mathcal{U}(\mathbb{Z}_n)| = \phi(n)$ donde $\phi : \mathbb{N} \to \mathbb{N}$ es la función de Euler, $\phi(n) = \#\{m \in \mathbb{N}$ con $m < n$ y $(m,n) = 1\}$.
25. Este ejercicio, entre otras cosas, muestra que la función de Euler es multiplicativa con respecto a los pares de números coprimos. Sean n y m dos números naturales coprimos, entonces

    (a) $\mathbb{Z}_{n.m} \cong \mathbb{Z}_n \oplus \mathbb{Z}_m$

    (b) $\mathrm{Hom}_{Gr}(\mathbb{Z}_n, \mathbb{Z}_m) = \mathrm{Hom}_{Gr}(\mathbb{Z}_m, \mathbb{Z}_n) = 0$

    (c) $\mathrm{Hom}_{Gr}(\mathbb{Z}_n \oplus \mathbb{Z}_m, \mathbb{Z}_n \oplus \mathbb{Z}_m) \cong \mathrm{Hom}_{Gr}(\mathbb{Z}_n, \mathbb{Z}_n) \oplus \mathrm{Hom}_{Gr}(\mathbb{Z}_m, \mathbb{Z}_m)$

    (d) $\mathrm{Aut}_{Gr}(\mathbb{Z}_{n.m}) \cong \mathrm{Aut}_{Gr}(\mathbb{Z}_n) \times \mathrm{Aut}_{Gr}(\mathbb{Z}_m)$

    (e) Concluir que $\phi(mn) = \phi(m)\phi(n)$ para todo par de numeros m, n con $(m,m) = 1$.

26. Sea G el grupo de transformaciones afines de $\mathbb{R}$, es decir, el grupo de funciones de la forma $x \mapsto a.x + b$ con $a \neq 0$. Ver que es efectivamente un grupo (encontrar inversos), y que es isomorfo al subgrupo de matrices inversibles formado por las matrices de la forma

    $$G \cong \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \text{ con } a, b \in \mathbb{R},\ a \neq 0 \right\}$$

    Ver que $G \cong (\mathbb{R},+) \rtimes (\mathbb{R} - \{0\}, .)$.
    Si se considera el grupo de transformaciones afines en $\mathbb{R}^n$, es decir, las transformaciones del tipo $x \mapsto A.x^t + v$ con $A \in GL_n(\mathbb{R})$ y $v \in \mathbb{R}^n$, ver que este grupo es isomorfo a $(\mathbb{R}^n,+) \rtimes GL_n(\mathbb{R})$.

27. Si $G = \mathbb{Z}_3$ y $X = \mathbb{R}^3$, ver que

$$\begin{array}{rcl} \overline{0}.(x,y,z) & = & (x,y,z) \\ \overline{1}.(x,y,z) & = & (y,z,x) \\ \overline{2}.(x,y,z) & = & (z,x,y) \end{array}$$

define una acción (lineal). Ver que el subespacio V generado por el vector $(1,1,1)$ es un subespacio "estable" por la acción de $\mathbb{Z}_3$, y la acción restringida a V es trivial. Ver que el complemento ortogonal de V (con respecto al producto interno canónico en $\mathbb{R}^3$) es estable por la acción de $\mathbb{Z}_3$ (aquí la acción no es trivial). Ver que $V^{\perp}$ no contiene subespacios propios $\mathbb{Z}_3$-estables.

28. Sea $G = \mathbb{Z}_4$ actuando en $\mathbb{R}^4$ por la fórmula

$$\overline{1}.(x,y,z,t) = (t,x,y,z)$$

descomponer a $\mathbb{R}^4$ en suma directa de subespacios $\mathbb{Z}_4$-estables lo "más chicos posible". (sugerencia: dado un subespacio estable buscar complementos con los ortogonales).

29. Sea $\mathcal{H}$ el grupo de Hamilton actuando sobre sí mismo por conjugación. Para cada elemento de $\mathcal{H}$ describir las órbitas. Separar las órbitas puntuales para así encontrar de nuevo el centro. Encontrar los "a_i" del teorema de la ecuación de clases y sus respectivos subgrupos $\mathcal{Z}(a_i)$.

30. Sea G un grupo finito, $|G| = p^n$ para algún número primo p, entonces el centro de G es no trivial, i.e. $|Z(G)| > 1$.

31. Sea G un grupo de orden p^2, entonces G es abeliano. Ver que si $|G| = p^2$ entonces $G \cong \mathbb{Z}_{p^2}$ o bien $G \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$. (por qué $\mathbb{Z}_{p^2} \not\cong \mathbb{Z}_p \oplus \mathbb{Z}_p$?).

32. Sea G un grupo no abeliano de orden p^3, entonces $Z(G) = [G,G]$ y $|Z(G)| = p$ (en particular es cíclico, y está generado por cualquiera de sus elementos salvo la identidad). Ver que el grupo de matrices de la forma $\left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \text{ con } a,b,c \in \mathbb{Z}_p \right\}$ es un ejemplo de grupo no abeliano de orden p^3. Describir en este caso $[G,G]$.

33. **Teoremas de Sylow**: Este ejercicio es una guia o esquema de demostración de los teoremas de Sylow, que son los siguientes:
Sea G un grupo finito, p un número primo, supongamos que $|G| = p^r.m$ donde $(p,m) = 1$.

- (1er teorema de Sylow) Existe por lo menos un subgrupo S de G tal que $|S| = p^r$. Un tal subgrupo se llamara un p-subgrupo de Sylow.
- (2do teorema de Sylow) Si S y S' son dos p-subgrupos de Sylow de G, entonces son conjugados.
- (3er teorema de Sylow) La cantidad de p-subgrupos de Sylow de G es un numero congruente a 1 modulo p.

Se propone el siguiente esquema:

1 Hacer induccion en el orden de G. Resolver primero el caso G conmutativo. Despues para el caso no conmutativo, separar a su vez el caso $|\mathcal{Z}(G)| = 1$ y $|\mathcal{Z}(G)| > 1$. Para el caso $|\mathcal{Z}(G)| > 1$ considerar el grupo (de orden estrictamente menor!) $G/\mathcal{Z}(G)$. Para el caso $|\mathcal{Z}(G)| = 1$, a partir de la ecuación de clases, deducir que existe un subgrupo $\mathcal{E}_i$ tal que $|\mathcal{E}_i| = p^r.m'$ con $m' < m$, y usar la hipotesis inductiva en $\mathcal{E}_i$.

2 Para el segundo teorema, también por induccion en G, seguir la misma estructura que en el 1er teorema, es decir, resolver primero el caso conmutativo, después suponer G no conmutativo y $|\mathcal{Z}(G)| > 1$ y considerar $G/\mathcal{Z}(G)$. Si p^r divide a $|\mathcal{Z}(G)|$ mostrar que todos los subgrupos de Sylow están incluidos en el centro. Sino, dados S y S' dos subgrupos de Sylow, considerar $\langle S, \mathcal{Z}(G)\rangle$ y demostar que tiene orden menor que G, y que S' está contenido en $\langle S, \mathcal{Z}(G)\rangle$. Finalmente si $|\mathcal{Z}(G)| = 1$ considerar el subgrupo $\mathcal{E}_i$ que provee la ecuación de clases.

3 Para el tercer teorema, considerar el conjunto $X = \{S/ \ S \text{ es } p\text{-subgrupo de Sylow de } G\}$. Como dos grupos conjugados son isomorfos, por lo tanto tienen el mismo orden, G actúa por conjugación en X, y a partir del teorema anterior la acción es transitiva. ...